European Agency of Digital Trust

Política de Emisión de Certificados de persona jurídica

Área Documental de Operaciones

Certificado	Sin dispositivo cualificado	Con dispositivo cualificado
Persona Jurídica (Identificación presencial)	1.3.6.1.4.1.501.2.1.1.**0**.41231	1.3.6.1.4.1.501.2.1.1.1.**1**.1231
Persona Jurídica (Identificación a distancia por videoconferencia)	1.3.6.1.4.1.501.2.1.1.**3**.41231	1.3.6.1.4.1.501.2.1.1.**4**.41231
Sello de Órgano	1.3.6.1.4.1.501.2.1.1.**0.41233**	1.3.6.1.4.1.501.2.1.1.**1.41233**

EADTrust Policy Committee
EADTRUST EUROPEAN AGENCY OF DIGITAL TRUST

Octubre de 2020
Versión 3

Nota sobre derechos de autor

Versiones del documento

Esta publicación podría incluir inexactitudes técnicas o errores tipográficos.

Según evoluciona el estado de la técnica y el contexto legislativo, puede ser necesario incluir cambios en este documento, por lo que se recomienda comprobar en la página web de EADTrust la última versión de la publicación.

European Agency of Digital Trust puede realizar mejoras y cambios en los productos y en los programas descritos en esta publicación en cualquier momento.

Certificación ISO 9001. ISO 27001 e ISO 20000-1

EADTrust ha superado diversas auditorías, y, en particular las relativas a las normas ISO 9001. ISO 27001 e ISO 20000-1, con el siguiente alcance:

El Sistema Integrado de Gestión de la Información que da soporte a consultoría, auditoría, desarrollo y provisión de los siguientes servicios electrónicos de confianza: Autoridades de Certificación (PKI) que cumplen los requerimientos de las normas EN 319 401 v2.2.1, EN 319 411-1 v1.2.2, EN 319 411-2 v2.2.2, EN 319 421 v1.1.1 para Sellado de Tiempo, Emisión de Certificados, Validación de OCSP, Firma Electrónica Centralizada, Extensión de Firma Electrónica, Notificación Electrónica Fehaciente (Correo Electrónico Certificado), Publicación Electrónica Fehaciente, Comprobación fehaciente de contenidos digitales, Foro Electrónico de Accionistas, Emisión y Gestión de Claves, Cartulario (Custodia Digital de Documentos Electrónicos), Custodia de Evidencias Electrónicas (Retención de Datos), Voto Electrónico, Facturación Electrónica, Digitalización Certificada, Gestión de firma manuscrita digitalizada y Gestión de firma avanzada vocal, para garantizar la validez legal de todo tipo de gestiones que las utilizan, de acuerdo a la declaración de aplicabilidad vigente.

Certificados

Norma	Certificado
ISO 20000-1:2011	10242586 / 10242587
ISO 27001:2013	10242584 / 10242585
ISO 9001:2015	10242588 / 10242589

Tabla de Contenidos

Control Documental

Esta sección refleja la información del documento, sus propiedades y el historial de versiones.

TABLA1. HISTORIAL DE VERSIONES.

Versión	Fecha	Documentos sustituidos	Descripción
1.0	25/11/19	Ninguno	Inicio en la prestación del servicio de emisión de certificados cualificados conforme al Reglamento (UE) 910/2014 eIDAS.
2.0	22/04/2020	1.0	Revisión y actualización de la política como parte del proceso de mejora continua e introducción de la videoconferencia como medio de identificación ante la RA.
3.0	28/10/2020	2.0	Se introducen los perfiles de certificado de sello de órgano alineados con el documento "Perfiles de Certificados Electrónicos 2.0" de la AAPP.

TABLA2. DATOS DEL DOCUMENTO.

Propiedades del documento.	
Propietario	EADTrust European Agency of Digital Trust, S.L.
Fecha	28 de octubre de 2020
Distribución	Público
Nombre / Código	OPR-PC- V3.0-Emisión_certificados_persona_jurídica_EADTrust

1.- Introducción

Este documento establece la Política de certificación que EADTrust European Agency of Digital Trust, S.L (en adelante, EADTrust), ha definido para la expedición de certificados cualificados de Persona Jurídica para la creación de sellos electrónicos cualficados y contempla:

- La creación, comprobación, validación y revocación de certificados cualificados de autenticación y sello electrónico de persona jurídica basándose en la identificación de documentos de identidad, tales como el pasaporte o el DNI del solicitante y en la documentación legal que acredita la representación.

Si el titular del certificado es una administración pública el certificado cualificado de Persona Jurídica se denomina "Certificado de Sello de Órgano".

La finalidad de esta política es definir las líneas generales de la prestación de este servicio. Para una información más detallada y completa se recomienda la lectura de la Declaración de Prácticas de Servicios Electrónicos de Confianza de EADTrust (en adelante DPC o Declaración de Practicas de Certificación).

1.1.- Definición

EADTrust ha definido sus prácticas y políticas según los requisitos del REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE (en adelante, eIDAS) y los estándares internacionales establecidos en ETSI.

Dentro de las políticas de certificación definidas en ETSI EN 319 411-1, EADTrust adopta como política de base para sus certificados, la denominada Política de Certificados Normalizados (NCP) que cumple con las mejores prácticas generales reconocidas para la emisión de certificados.

Este documento abarca además la variación de política definida en ETSI como política de certificados normalizados ampliada (NCP+) para su uso en certificados cualificados con un dispositivo criptográfico seguro (firma o descifrado).

Asimismo, para los certificados cualificados de persona jurídica conforme al Reglamento (UE) No 910/2014, EADTrust adopta las variaciones de política definidas en la norma ETSI EN 319 411-2:

- Política para el certificado cualificado de la UE expedido a una persona jurídica (QCP-l) y;
- Política para el certificado cualificado de la UE emitido a una persona jurídica cuando la clave privada y el certificado correspondiente residen en un QSCD (QCP-l-QSCD).

Para el certificado de Sello de Órgano, se ha tomado en consideración, además, lo establecido en el documento denominado "Perfiles de Certificados Electrónicos 2.0 en el marco de la Leyes españolas 39/2015 y 40/2015." [1]

Para más detalles consultar los perfiles de certificados y el soporte y niveles de seguridad descritos en este documento.

[1] https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

1.2.- Soporte y nivel de seguridad

Tipo de Certificado: Entidad legal / Persona Jurídica / Entidad sin personalidad Jurídica / Sello de Órgano

Certificado	Standard Policy Identifier	EAD Trust Policy OID	Formato	Nivel de seguridad
Sello Corporativo	No se indica Política asociada a RFC3161	1.3.6.1.4.1.501.2.1.1.0.3161	Software Dispositivo *	No cualificado Distancia***
Sello Corporativo	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.**0.**41231	Software	Sustancial Presencial**
	0.4.0.194112.1.3 (OID ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.**1.**41231	Dispositivo*	Alto Presencial**
	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.**3.**41231	Software	Sustancial Distancia***
	0.4.0.194112.1.3 (OID ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.**4.**41231	Dispositivo*	Alto Distancia***
Sello de órgano	0.4.0.194112.1.1 (OID ETSI QCP-l)	1.3.6.1.4.1.501.2.1.1.**0.**41233	Software	Sustancial Presencial**
	0.4.0.194112.1.3 (OID ETSI QCP-l-QSCD)	1.3.6.1.4.1.501.2.1.1.**1.**41233	Dispositivo*	Alto Presencial**

(*) Los dispositivos habituales son HSM (Hardware Security Module), token seguro y tarjeta chip. Los tokens USB se consideran equivalentes al uso de tarjetas inteligentes contando con que incorporan el lector de tarjeta en el mismo encapsulado.
(**) Presencial: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza de manera presencial en las instalaciones de la RA.
(***) Distancia: Identifica los OID de Políticas de certificados en los que la validación y autenticación de la identidad del Solicitante se realiza por la RA, de manera remota (on line también denominada telepresencia). Para ello pueden desplegarse medios de videoidentificación o videoconferencia.

2.- Participantes en la PKI

2.1.- Autoridades de Certificación

Las CAs de EADTrust se organizan en una jerarquía de dos niveles, con diferentes roots, adaptadas a las normas actuales y las mejores prácticas del sector. Se diferencian por algoritmo de clave pública, tamaño de la clave y por diferentes usos de los certificados de entidad final, cualificados y no cualificados.

EADTrust dispone para certificados cualificados

- RSA Root CA 2048-bit key size with SHA256 digest algorithm para certificados cualificados.
- RSA Root CA 4096-bit key size with SHA256 digest algorithm para certificados cualificados.
- RSA Root CA 8192-bit key size with SHA512 digest algorithm para certificados cualificados.
- ECC Root CA P-256 with SHA256 digest algorithm para certificados cualificados.
- ECCRoot CA P-384 with SHA384 digest algorithm para certificados cualificados.

Para certificados no cualificados

- RSA Root CA 2048-bit key size with SHA256 digest algorithm para certificados No cualificados.

Para proporcionar un nivel de seguridad adecuado, las CAs raíz siempre se mantienen offline, emitiéndose los certificados para los subscriptores, desde las Sub-CAs correspondientes.

Pueden emitir Certificados bajo la jerarquía EADTrust las Autoridades de Certificación operadas por organizaciones externas cuyas Políticas o DPC (CPS) estén conformes con las Política de Certificación contempladas en su DPC (CPS) y

hayan sido previamente autorizadas. Existirá una relación escrita formal y contractual con EADTrust para dar cobertura a los compromisos mutuos.

Normalmente, cada raíz de EADTrust cuenta con una o dos CAs intermedias para emisión de certificados de entidad final para suscriptores.

Cada CA firma su propia CRL y las respuestas OCSP se firman por la SubCA correspondiente. El propio certificado de entidad final contiene la información del endpoint en el que se obtiene la CRL o al que se puede consultar el servicio OCSP. Existe un perfil de certificado OCSP de uso opcional para servidores OCSP externos.

2.2.- Autoridades de Registro

EADTrust, como CA, emite algunos certificados directamente. Sin embargo, como empresa de servicios, realiza la gestión de las solicitudes y emisión de los certificados a través de sus Autoridades de Registro - RAs

Estas RAs son entidades que actúan de acuerdo con esta Política de Certificación de EADTrust, y que reflejan en una relación escrita formal y contractual con EADTrust. Su objetivo principal es la gestión de relaciones de suscriptores, que incluye la identificación y registro de los suscriptores, las solicitudes de certificados y cualquier otra obligación indicada en esta política y las políticas específicas de certificados en relación con la gestión del ciclo de vida de los certificados.

Hay dos formas principales que la RA puede adoptar en la estructura de EADTrust respecto a la verificación de identidad de los solicitantes

- inscripción en persona con personación ante una agente de RA
- inscripción a distancia, en las variantes siguientes:
  - videoconferencia (también descrita como telepresencia) o videograbación verificada.
  - Alternativamente *Firma Electrónica Cualificada* (aseguramiento sustancial o alto) En el caso en el que se utiliza una firma electrónica cualificada como parte de una solicitud de certificado.

El primer mecanismo de identificación a distancia nos permite video identificar a la persona física con documento físico. El segundo mecanismo nos permite identificar a la persona física que ya dispone de un certificado electrónico y usar el mismo nivel de aseguramiento que el certificado emitido para otras tipologías de certificados.

Para la videoconferencia[2] EADTrust cumple lo establecido en el Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente al COVID-19. Así como, lo previsto en la normativa española publicada por el servicio de prevención de Blanqueo de Capitales (SEPBLAC) y la Directiva (UE) 2015/2366 (PSD2) que se utilizará incluso en los servicios de iniciación de pagos como medio para proporcionar autenticación fuerte de los clientes.

Para más detalles se recomienda la lectura de la política definida al efecto.

Tanto si la suscripción es en persona o mediante telepresencia, cada RA está sujeta, pero no limitada, a las siguientes obligaciones.

Cada RA está sujeta, a las siguientes obligaciones:

- Identificación y autenticación de los titulares y suscriptores de certificados.
- Desarrollo de una relación contractual para la emisión de certificados con la entidad final o el suscriptor.
- Solicita la generación de certificado (por medio de comunicación autenticada con la CA online) entrega del certificado en un dispositivo cualificado de creación de sello (si es el caso) o mediante fichero cuando no se requiera dispositivo cualificado de creación de sello. SI se comprueba por parte de la RA o un auditor que una solicitud de certificado (PKCS#10) se ha generado en un dispositivo criptográfica adecuado (QSCD) se emitirá el certificado en soporte de fichero para permitir su inserción en el QSCD.
- Conservación de cualquier documentación relevante y relacionada con la emisión del certificado o con la

[2] http://www.sepblac.es/espanol/sujetos_obligados/autorizacion_identificacion_mediante_videoconferencia.pdf.

relación del suscriptor con la RA.

- Proporcionar cualquier información requerida por EADTrust relacionada con sus servicios de gestión de identificación de la entidad y gestión de la entrega de los certificados en las modalidades determinadas en la solicitud, en cualquier momento, y, especialmente, durante la evaluación de cumplimiento anual con las Políticas de Certificación de EADTrust.

El período de conservación para cualquier documentación es de 15 años, excepto en aquellos casos en los que se especifique un período de conservación más corto en la política del certificado.

Las RAs que cooperan en la jerarquía de EADTrust, están obligadas a cumplir con todas las Políticas de Certificación de EADTrust, así como superar la evaluación anual de cumplimiento obligatoria realizada por EADTrust o cualquier tercero evaluador o auditor designado por EADTrust.

2.3.- Suscriptores (titulares de certificado)

Entidades Finales

Las entidades finales son personas jurídicas o entidades sin personalidad jurídica que reciban servicios de emisión y confíen en certificados de EADTrust. Los certificados de Sello Electrónico se emiten a

- Solicitantes de certificados, por sí mismos o cualquier otro interesado.
- Suscriptores de certificados que tienen la propiedad del certificado.
- Propietarios de la clave, quienes las utilizan para los propósitos específicos del certificado.
- Terceros que confíen en los certificados.

Solicitantes de Certificados

Los solicitantes de certificados pueden ser Personas Físicsa con capacidad para actuar en nombre de la entidad que solicita el certificado de Sello Electrónico de Entidad o de sello de Órgano.

Los **certificados de** Sello de Órgano. los pueden solicitar funcionarios de las administraciones públicas que acrediten su identidad y su adscripción al organismo para el que solicitan el certificado.

En caso de concursos y licitaciones, los certificados de Sello de Órgano los pueden solicitar las personas designadas en cumplimiento de los pliegos por el poder adjudicador.

Suscriptores del Certificado

El suscriptor de un certificado es la persona jurídica, entidad u organización que posee el certificado que se vincula con una clave privada.

Propietarios de la clave

El propietario de la clave es una persona física, representante o empleado autorizado por la organización puede utilizar exclusivamente las claves criptográficas del certificado.

Incluso si el propietario de la clave suele ser identificado como el firmante en la regulación de la firma electrónica, se designa por su clasificación más genérica, para incluir cualquier otro uso del certificado (como la autenticación o el descifrado).

La capacidad del propietario de la clave y el alcance para actuar y operar en lugar del suscriptor real se especificarán, en cada caso, en el certificado, cumpliendo con los requisitos establecidos en esta esta política y en la DPC (CPS)

Partes que Confían

Las entidades o individuos que actúan confiando en certificados u objetos sellados emitidos bajo esta PKI son partes que confían.

Las partes que confían pueden o no ser suscriptores dentro de esta PKI, pero, en cualquier caso, se proporcionarán diferentes canales de comunicación, para que puedan (como deberían) verificar la validez del certificado y su propósito.

Deben comprobar por el campo AIA (Authority Information Access) de los certificados que pueden reconstruir la cadena de confianza desde el certificado de entidad final hasta la autoridad Raiz, y que pueden indentificar el punto de consulta de validez de certificados por el servicio OCSP, o, cuando corresponda, por la lista CRL.

En el caso de los certificados cualificados, deben poder identificar las autoridades incluidas en las listas de confianza TSL administradas por el Organismo de Supervisión correspondiente al país, en España la Secretaría de Estado para el Avance Digital adscrita al Ministerio de Economía y Empresa[3] y por el organismo europeo que consolida las TSL nacionales[4].

Las partes que confían deben conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas. Un resumen de lo que deben conocer se encuentra disponible en el documento PDS (PKI Disclosure Statement), redactado de forma que se facilite la divulgación de los servicios con lenguaje sencillo de forma similar al prospecto de un medicamento.

- www.policy.eadtrust.eu/pds/

3.- Uso del certificado

A continuación, se describen los usos permitidos y prohibidos de los certificados emitidos por EADTrust.

3.1.- Usos Adecuados del Certificado

Los certificados de sello electrónico cualificados garantizan la identidad del suscriptor y del titular de la clave privada. Cuando se utilizan con dispositivos cualificados de creación de sellos, son adecuados para ofrecer soporte al sello electrónico cualificado. Los certificados de sello de órgano se utilizan en el marco de la gestión de las Administraciones Publicas, y permiten la identificación y autenticación del ejercicio de la competencia de la AAPP, órgano, o entidad actuante y el cifrado de datos.

Los certificados cualificados se ajustan a la norma técnica En 319 412 (documentos 1 a 5) del Instituto Europeo de Normas de Telecomunicaciones ETSI.

Si los certificados se emiten a personas jurídicas o entidades sin personalidad jurídica al objeto de crear sellos electrónicos se establecen consideraciones equivalentes a las de las firmas electrónicas, lo que da lugar a los sellos electrónicos avanzados basados en certificados cualificados y cuando estos se gestionan haciendo uso de dispositivos cualificados de creación de sello, a los sellos electrónicos cualificados.

En el caso de los sellos de tiempo cualificados, es requisito del Reglamento eIDAS que se creen haciendo uso de firmas avanzadas lo que permite que estas estén basadas o no en certificados cualificados. EADTrust contempla en su servicio de sello de tiempo cualificado la posibilidad de usar ambos tipos de certificados.

3.2.- Usos Prohibidos del Certificado

Los certificados deberán utilizarse para el fin específico para el que fueron creados. Asimismo, los certificados sólo deben utilizarse de conformidad con la legislación aplicable.

[3] https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl
[4] https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Los Certificados no se pueden usar en equipos de control destinados su utilización en situaciones peligrosas o en los que un mal funcionamiento suponga un peligro para la vida humana o para objetos valiosos. Cualquier uso en estos contextos exime de responsabilidad al Prestador de servicios de confianza digital.

EADTrust incorpora en el certificado información sobre la limitación de uso, en campos estandarizados en los atributos "uso de la clave" (**Key usage**), "uso extendido de clave" (**Extended Key Usage**).

4.- Administración de Políticas

4.1.- Organización que Administra el Documento

EADTrust, con domicilio social en Calle Alba, 15 de Madrid (España) y NIF. B-85626240, es la Autoridad de Certificación que emite los certificados que corresponden a esta Política de Certificación.

4.2.- Contacto

Nombre del PSC	European Agency of digital Trust, S. L.
Dirección	C/ Alba,15, 28043 Madrid - Spain
Dirección de email	policy@eadtrust.eu
Teléfono	(+34) 902365612 / (+34) 917160555

4.3.- Procedimiento de aprobación de las políticas de certificados

El Órgano de Aprobación y Gestión de Políticas de Certificación de EADTrust aprueba los cambios finales realizados en este documento una vez que determine que cumplen con los requisitos establecidos.

Es posible contactar con el Órgano de Gestión y Aprobación de Políticas de certificados en: E- mail: policy@eadtrust.eu.

Las direcciones postales, teléfonos y fax se encuentran publicadas en www.eadtrust.eu.

5.- Publicación de información y repositorio de certificados

5.1.- Publicación de la información de certificación

La CA divulga públicamente sus Políticas de Certificados y la Declaración de Prácticas de Certificación a través de su web (un medio on line apropiado y fácilmente accesible que está disponible 24 horas al día, 7 días a la semana). EADTrust divulga públicamente sus prácticas empresariales de Certificación en la medida requerida por el esquema de auditoría seleccionado de la CA (ver Sección "Auditoría de cumplimiento y otras evaluaciones").

La URL en la que está disponible la información de políticas y la Declaración de Prácticas de Certificación es:

- policy.eadtrust.eu

La divulgación incluye todo el material requerido por la norma RFC 3647 y se estructura de acuerdo con dicha norma.

5.2.- Tiempo o Frecuencia de Publicación

EADTrust se compromete a desarrollar, implementar, hacer cumplir y actualizar con periodicidad bienal, su Política de Certificación y su Declaración de Prácticas de Certificación, como uno de los elementos asociados a la auditoría bienal. El intervalo de actualización será menor cuando se produzcan cambios técnicos o legales que hagan necesaria una actualización.

5.3.- Repositorios

La CA proporciona información de revocación para los Certificados Subordinados y los Certificados de Suscriptor disponibles de acuerdo con esta Política.

La URL en la que está disponible la información de revocación (y que se indica en el campo AIA del certificado) es:

- ocsp.eadtrust.eu

Además, la posible revocación de las CA raíz y las CAs subordinadas quedará registrada en la URL:

- crl.eadtrust.eu

Las políticas de certificación, la declaración de prácticas de certificación y la declaración abreviada para terceros que confían (PDS, Policiy Disclosure Statement) estarán disponles en la URL:

- policy.eadtrust.eu

6.- Identificación y Autenticación

6.1.- Nombre

6.1.1.- Tipos de Nombres

Todos los certificados de usuario de entidad final contienen un nombre dado en el campo **Subject Name**. Los atributos especificados en el nombre diferenciado en el campo de Sujeto están contenidos en la sección correspondiente al perfil de certificado. El valor autenticado en el campo **Common Name** es el nombre del propietario de la clave. El campo **subjectAltName** también se utiliza ocasionalmente para situar un nombre que se puede utilizar para identificar el sujeto, pero que es diferente del nombre que aparece en el campo **Subject Name**.

En relación con los Subject (sujeto al que se emite el certificado) se considera los siguientes campos:

- Country: ES (corresponde al código ISO de país, correspondiente al Estado Español).
- Organizational Unit Name: El nombre del tipo de servicio de certificación que se presta.
- Surname: Los apellidos del suscriptor, autorizado por la Entidad de Registro.
- Given Name: El nombre del suscriptor, autorizado por la Entidad de Registro.
- Serial Number: DNI/NIE, del suscriptor, autorizado por la Entidad de Registro, u otro número descrito en la norma EN 319 412-1.
- Common Name: El nombre en texto libre del suscriptor, autorizado por la Entidad de Registro.

El perfil de los certificados se puede solicitar a través del servicio de soporte al cliente de EADTrust aunque estarán disponibles en la sección de políticas disponle en la URL:

- policy.eadtrust.eu

La estructura sintáctica y el contenido de los campos de cada certificado emitido por EADTrust, así como su significado semántico, se encuentran descritos en cada uno de los perfiles de certificados.

6.1.2.- Persona Jurídica:

En certificados correspondientes a personas jurídicas, esta identificación se realizará por medio de su denominación o razón social, y su identificación fiscal u otro número de identificación de los admitidos en la norma EN 319 412-1. Necesidad de que los nombres sean significativos

El nombre del sujeto y el emisor contenidos en un certificado, deben ser significativos en el sentido de que la CA tenga evidencia de la asociación existente entre estos nombres y las entidades a las cuales pertenecen.

Cada certificado digital contiene un conjunto único de atributos de nombre único. Estos atributos incluyen una recopilación del nombre de la persona, nombre de la compañía, unidad organizacional e identificador único.

Los certificados de sello de órgano son un caso particular de este tipo de certificados y tienen un perfil propio.

6.1.3.- Tratamientos de datos excluidos en los certificados

No se harán constar en los certificados datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo cuando alguno de los datos sea de consignación obligatoria por una normativa aplicable.

Cuando sean de aplicación las excepciones previstas en el artículo 9.2 del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se actualizará la presente Política, para especificar de manera clara la excepción aplicada y la razón por la que se lleva a cabo.

6.1.4.- Normas para interpretar diferentes formas de nombres

EADTrust atiende a lo estipulado por el estándar X.500 de referencia en la ISO/IEC 9594 **Informationtechnology – Open SystemsInterconnection – TheDirectory: Public-key and attribute certificate frameworks**

- X.509 - ISO/IEC 9594-813
- X.520 -ISO/IEC 9594-614

6.1.5.- Singularidad de los nombres

Los nombres de suscriptores y, en su caso, los nombres de los titulares de los certificados (considerando los diferentes atributos) son únicos para cada tipo de certificado dentro de la Declaración de prácticas de certificación de EADTrust.

6.2.- Validación inicial de la identidad

6.2.1.- Método para probar la posesión de la clave privada

Cuando se genera un par de claves por la CA a instancias de la RA:

- si las claves se almacenan en un token o una tarjeta criptográfica, la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del token o de la tarjeta criptográfica y del correspondiente certificado y el par de claves almacenados en su interior. De no ser preciso el uso de Dispositivo, los ficheros que contienen el certificado y la clave los entrega la Autoridad de registro de forma separada a la contraseña que permite su uso. Si las claves se entregan en un fichero PKCS#12 (o PFX) la prueba de posesión de la clave privada se demuestra en virtud del procedimiento confiable de entrega y aceptación del fichero y de la clave de descifrado, que podrán hacer uso de técnicas de comunicación de doble factor de

autenticación (por ejemplo, un mensaje de correo electrónico o un SMS) o un secreto compartido determinado en el momento de completar la solicitud de certificado.

Cuando se genera el par de claves por el solicitante:

- Por el propietario clave, la posesión de la clave privada se demuestra por la entrega de la solicitud PKCS#10 a la Autoridad de Registro. El solicitante debe aportar un informe de auditor que confirme que realmente se ha generado la clave dentro de un HSM, salvo que el personal de la RA tenga la posibilidad de comprobar por si mismo que la solicitud PKCS#10 se ha generado en un HSM.

6.2.2.- Autenticación de la organización

Como parte del proceso de autenticación de EADTrust, en el caso de expedición de certificados de persona jurídica, o de sello de órgano se valida el nombre de la organización introducido durante la inscripción, que se hace constar en el campo apropiado del certificado.

La organización a la que se atribuye un certificado debe ser una entidad activa, confirmada por una autoridad oficial responsable del registro de empresas dentro de la jurisdicción específica (localidad, estado, país) indicada en la solicitud del certificado. El nombre de la organización inscrita y el nombre alegado deben coincidir literalmente. En caso de existir abreviaturas, solo se aplicarán a las partes que identifican el tipo legal de sociedad o entidad (S.A., S.L., S. COOP., LLC, Ltd). Cuando las entidades no sean sociedades se utilizarán de referencia los poderes notariales aportados y publicaciones de nombramientos en los boletines oficiales.

En el caso de certificados emitidos a Prestadores de Servicios contemplados en las Directivas de Pagos, se constatará su existencia en el Registro administrado por el Órgano Supervisor (Competent Authorities).

Los certificados de sello de órgano son un caso particular de este tipo de certificados y están destinados a órganos de la administración pública.

En el caso de licitaciones, se tendrán en cuenta las condiciones establecidas en los pliegos por el poder adjudicador.

6.2.3.- Autenticación de la identidad individual

La identificación de los suscriptores se llevará a cabo mediante Entidades de Registro propias o afiliadas, comprobando los documentos de identidad y de representación, mediante personación del titular del certificado o mediante identificación a distancia por videoconferencia

El día de la cita, el solicitante deberá asistir con los documentos que soportan su solicitud, vigentes y en buen estado de conservación. Los documentos a presentar son los siguientes:

- Documento de Identificación de la persona física: DNI, NIE, PAS
- Poder notarial, que acredita la Representación vigente
- Una declaración jurada de que el poder es vigente y no ha sido revocado con anterioridad.

Debe conocer además la siguiente información:

a) No. De identificación de la entidad (CIF/NIF)
b) Datos del domicilio de la entidad
c) Teléfonos y e-mail de contacto con los directivos de la entidad
d) Copia de los estatutos de creación de la entidad. .

La RA podrá realizar comprobaciones adicionales como consultas a bases de datos que contengan información publicada en el BORME.

En el caso de licitaciones, se tendrán en cuenta las condiciones establecidas en los pliegos por el poder adjudicador.

6.3.- Identificación y autenticación para la solicitud de revocación

El inicio de una solicitud de revocación se produce:

- A solicitud de un representante legal o designado de la entidad suscriptora del certificado en la que prestaba servicios el titular del certificado,
- Por el titular, por compromiso de sus claves o por cualquier otra razón que lo requiera.

Para solicitar la revocación se requiere la personación física del solicitante de la revocación en una Entidad de Registro, o bien que el solicitante haga uso del servicio de revocación remota proporcionado al efecto, que podrá requerir la aportación de información específica para ello.

7.- Requisitos Operacionales del Ciclo de Vida de los Certificados

7.1.- Solicitud del Certificado

El interesado en un certificado de los definidos en esta política deberá cumplimentar el formulario de solicitud de emisión certificados disponible en la página web www.eadtrust.eu.

En el citado formulario, podrá agendar, además, una cita con la Autoridad de Registro de EADTrust para la verificación de su identidad.

La cita con la Autoridad de Registro de EADTrust se podrá llevar a cabo mediante personación en la Autoridad de Registro de EADTrust, o mediante verificación de identidad a distancia (identificación remota) por videoconferencia o por firma electrónica cualificada, conforme a los requisitos definidos en la Política específica definida por EADTrust al efecto.

Una vez cumplimentado el formulario de solicitud, EADTrust enviará un e mail con la información de la fecha y hora de la cita; así como de la documentación que deberá aportar o enviar a la RA antes de la fecha de la cita agendada.

La documentación deberá estar actualizada y vigente. Los documentos que se envíen digitalizados deberán ser legibles.

De optar por la modalidad presencial de verificación de la identidad, los documentos que deberán aportarse deberán ser originales.

El solicitante del certificado indicará además si desea obtener certificados en soportes QSCD o en otro soporte admitido en esta política. También podrá indicar preferencias respecto a la longitud de las claves de firma que desea sean empleadas.
Cuando el solicitante quiera utilizar una clave generada por el mismo en un QSCD y con un certificado emitido por EADTrust, deberá aportar la clave privada en un PKCS#10.

En el caso de licitaciones, se tendrán en cuenta las condiciones establecidas en los pliegos por el poder adjudicador.

7.1.1.- Quién puede enviar una solicitud del certificado

Pueden solicitar un certificado de persona jurídica sus representantes, para:

- Autenticar la identidad de un usuario, de forma electrónica, ante terceros
- Sellar documentos o transacciones digitalmente de forma que se garantice la integridad de los datos trasmitidos y su procedencia.
- Cifrar datos para que solo el destinatario del documento pueda acceder a su contenido. En este caso, es recomendable contar con un procedimiento de respaldo de claves privadas, dado que, si se produjera alguna incidencia con ellas, EADTrust no tiene posibilidad de proporcionarlas.
- Los representantes de personas jurídicas que requieran realizar sellos digitales o sello de órgano.

7.1.2.- Proceso de inscripción y responsabilidades

Las tareas de identificación y validación de la información en el certificado y validación y aprobación de las solicitudes de emisión, revocación y renovación serán realizadas por las Oficinas de Registro propias y de la Autoridades de Registro.

Las Oficinas de Registro Propias de EADTrust o de las entidades usuarias con las que EADTrust firme el correspondiente instrumento legal deberán asumir las siguientes obligaciones:

- Validar la identidad y otros detalles personales del solicitante, del suscriptor y del propietario de la clave en los certificados o la información relevante para el fin de los certificados según estos procedimientos.
- Mantener toda la información y documentación relativa a los certificados, y gestionar su emisión, renovación, revocación o reactivación.
- Notificar a EADTrust sobre las solicitudes de revocación de certificados con la debida diligencia y de una manera rápida y confiable.
- Permitir a EADTrust el acceso a sus archivos de procedimiento y registros de auditoría para desempeñar sus funciones y mantener la información necesaria.
- Informar a EADTrust sobre las solicitudes de emisión, renovación, reactivación y cualquier otro aspecto relacionado con los certificados emitidos por EADTrust.
- Validar, con la debida diligencia, las circunstancias de revocación que puedan afectar a la validez del certificado.
- Cumplir con los procedimientos establecidos por EADTrust y con la legislación vigente en esta materia, en sus operaciones de gestión relacionadas con la emisión, renovación y revocación de certificados.
- Cuando proceda, puede realizar la función de poner a disposición del titular de la clave los procedimientos técnicos para la creación de firmas (clave privada) y la comprobación de la firma electrónica (clave pública).

7.2.- Procedimiento de Solicitud del Certificado

Una vez haya tenido lugar una petición de certificado y se ha agendado la cita conforme indica esta Política el operador de la RA procederá a iniciar el proceso de identificación y validación de identidad declarada.

El proceso se llevará a cabo en una plataforma de gestión interna. En esta la RA introduce los datos declarados y posteriormente verificará que la información proporcionada es correcta.

7.2.1.- Realización de funciones de identificación y autenticación

Es responsabilidad de EADTrust llevar a cabo correctamente la identificación del suscriptor. Este proceso se lleva a cabo antes de la emisión del certificado.

En todos los casos, los usuarios deben consultar la documentación específica de cada certificado para obtener detalles sobre cada uno de ellos.

Tras comprobar la identidad del solicitante por su DNI o documento de identificación, los operadores de la RA deberán leer y valorar la copia de los estatutos de la sociedad, de los poderes de representación y la declaración de que se encuentran vigentes, para confirmar que procede la emisión del certificado, considerando, entre otros aspectos que la solicitud de certificados se encuentra dentro de las potestades del solicitante.

En el caso de licitaciones se tendrán en cuenta las condiciones establecidas en los pliegos por el poder adjudicador.

7.2.2.- Aprobación o Rechazo de Solicitudes de Certificado

Una vez que se haya solicitado el certificado, la RA comprobará la información proporcionada por el solicitante, incluida la validación de la identidad del suscriptor, y de la suficiencia de poderes de representación.

Si la información no es correcta, la RA denegará la solicitud y se pondrá en contacto con el solicitante para explicar la razón. Si la información es correcta, se emitirá el certificado. Si la información es correcta, la RA solicitará la aprobación y con ella la emisión del certificado.

En el proceso de expedición de certificados de EADTrust, se aplican controles duales, de modo que la decisión de expedición del certificado no la pueda tomar la misma persona que comprueba la información asociada a la solicitud.

7.2.3.- Tiempo para procesar las solicitudes de certificado

Una vez verificada la información requerida en el proceso de solicitud de certificados, se podrá proceder a la emisión del certificado que se requiera. El tiempo estimado de emisión de certificados tras la verificación es de 24 horas en días laborables.

7.3.- Emisión del Certificado

Todas las solicitudes deben ser aprobadas en su totalidad antes de que los certificados puedan ser emitidos. Una vez aprobada la solicitud EADTrust emitirá el certificado y lo entregará personalmente o lo remitirá por vía telemática.

7.3.1.- Acciones de la CA durante la emisión del certificado

Los certificados se pueden emitir en un token criptográfico, en una tarjeta inteligente, en HSM o en un soporte de software.

Cuando no es un certificado basado en QSCD, EADTrust podrá entregar el certificado en un soporte de software USB, o enviarlo por email, adjuntando el certificado en un archivo .zip

I. Procedimiento de emisión de certificados expedidos en un token criptográfico o en una tarjeta inteligente:

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Tras la autenticación, la Autoridad de Registro solicita un certificado de EADTrust.
- Después de comprobar que la solicitud procede de una Autoridad de Registro autorizada, EADTrust emite el certificado de acuerdo con los procedimientos establecidos y lo envía a la Autoridad de Registro.
- Después de que la Autoridad de Registro haya comprobado que la solicitud proviene de EADTrust, descarga el certificado al dispositivo de creación de firmas usando un proceso seguro de administración de dispositivos criptográficos. En caso de que EADTrust provea un servicio de firma electrónica remota en nombre del firmante la inserción del material criptográfico se realizará en el dispositivo administrado por EADTrust y se entregarán al solicitante los medios de identificación que permiten su uso.
- Si EADTrust decide no emitir el certificado (incluso cuando los procedimientos de autenticación sean correctos), se notificarán al solicitante las razones de la decisión.

II. Procedimiento de emisión de certificados expedidos en un HSM:

- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante, y audita la generación de la solicitud de certificado en HSM y la solicitud de certificado con formato PKCS#10. También podrá admitirse un informe de auditoría de un especialista certificando que la solicitud se ha generado en un HSM.
- Tras la autenticación, la Autoridad de Registro solicita el certificado de EADTrust, aportando el fichero en formato PKCS#10.
- Después de comprobar que la solicitud procede de una Autoridad de Registro autorizada, EADTrust emite el certificado según los procedimientos establecidos y lo envía a la Autoridad de Registro

- Después de que la Autoridad de Registro haya comprobado que la solicitud proviene de EADTrust, esta descarga el certificado y lo pone a disposición del solicitante que deberá insertarlos en el dispositivo criptográfico en el que se generó la solicitud.
- Si EADTrust decide no emitir el certificado (incluso cuando los procedimientos de autenticación sean correctos), se notificarán al solicitante los motivos de la decisión.

III. Procedimiento de emisión de certificados emitidos mediante un mecanismo de software, con clave privada generada por el solicitante:

- Junto con el formulario de solicitud, el solicitante genera un par de claves en su propio ordenador, y hace llegar a EADTrust la solicitud de certificado con formato PKCS#10.
- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado, que se deberá insertar en el dispositivo en el que se generó la solicitud.
- No se admitirá ninguna clave pública que haya sido previamente usada para emitir un certificado en EADTrust

IV. Procedimiento de emisión de certificados emitidos mediante un mecanismo de software, con clave privada generada por el Prestador:

- El solicitante genera el formulario de solicitud.
- La Autoridad de Registro autentica la validez de la documentación presentada por el solicitante.
- Después de recibir la documentación, EADTrust emite el certificado vinculado con la clave privada, en formato PKCS#12 cifrado, que se puede insertar en cualquier dispositivo, incluso aunque no sea el dispositivo en el que se generó la solicitud.
- Por una vía diferente a la de la entrega del fichero PKCS#12 se hace llegar al solicitante la clave que permite el descifrado e instalación del fichero PKCS#12.
- EADTrust elimina la clave privada y el fichero PKCS#12 tras su remisión al solicitante.

7.3.2.- Notificación al suscriptor sobre la emisión del certificado por la CA

Cuando el suscriptor coincide con el titular de las claves, EADTrust realiza la notificación de la emisión en el mismo acto de firma del contrato de condiciones generales y particulares del servicio. Además, se entrega el dispositivo que almacena el certificado.

Cuando el suscriptor del certificado no es la misma persona que el titular de las claves (en certificados de representante de persona jurídica, funcionario público y otros relacionados con persona jurídica); EADTrust firma el contrato y entrega el dispositivo al titular de las claves y; adicionalmente envía una notificación certificada de la entrega al suscriptor.

7.4.- Aceptación del Certificado

La aceptación del certificado se produce al momento de la firma del contrato de términos y condiciones del servicio. No obstante, el suscriptor/titular del certificado dispone de 10 días hábiles desde la entrega del certificado para asegurarse de que funciona correctamente y, si es necesario, comunicar a EADTrust los defectos de funcionamiento.

Únicamente, si los defectos del certificado se debieran a causas técnicas (por ejemplo, funcionamiento defectuoso del almacenamiento en soportes de los certificados, problemas con la compatibilidad del programa, error técnico en el certificado, etc.) o a errores en los datos contenidos en el certificado aplicables a EADTrust, EADTrust revocará el certificado emitido y emitirá uno nuevo.

7.4.1.- Conducta que constituye la aceptación del certificado

Con la firma del contrato de condiciones generales y particulares del servicio, EADTrust entiende que el Suscriptor/Titular de las claves ha aceptado las condiciones de uso, obligaciones y deberes especificadas en el propio clausulado del contrato y por ende ha aceptado el certificado.

7.4.2.- Publicación del certificado por la CA

No se publican en directorios LDAP ni en otros repositorios los certificados expedidos a personas físicas para firma digital y autenticación ni a personas jurídicas para sello digital y autenticación.

7.4.3.- Notificación de la emisión del certificado por la CA a otras entidades

No aplica en el caso de personas jurídicas cuando no se emiten certificados para sitios web.

7.5.- Par de Claves y Uso del Certificado

7.5.1.- Clave privada del suscriptor y uso del certificado

El suscriptor que tiene la custodia de las claves:

- Garantizará el uso correcto y el mantenimiento de los soportes de almacenamiento del certificado.
- Facilitará a EADTrust y a sus entidades de registro información completa y adecuada, conforme a los requerimientos de esta política de certificado y de las políticas específicas, en especial en lo relativo al procedimiento de registro.
- Hará uso adecuado del certificado y, en particular, cumplirá con las limitaciones de uso del mismo.
- Salvaguardará diligentemente la clave privada (sea cual sea su soporte, e incluso si se trata de una copia de respaldo) y la clave o código PIN que permite su activación para evitar el uso no autorizado
- Notificará a EADTrust, y a cualquier otra persona que el suscriptor piense que pueda confiar en el certificado, sin demora razonable, si se produce alguna de las siguientes situaciones:
    - La clave privada del suscriptor se ha perdido, ha sido robada o se ha visto potencialmente comprometida.
    - El control sobre la clave privada del suscriptor se ha perdido debido a que los datos de activación se han visto comprometidos (por ejemplo, código PIN del dispositivo criptográfico) o debido a otras razones.
    - Inexactitud o cambios en el contenido del certificado, según lo notificado o sospechado por el suscriptor, solicitando la revocación del certificado cuando tales cambios constituyan una causa de revocación.
- Dejará de usar la clave privada al final del período de validez del certificado.
- Se abstendrá de supervisar, interferir o realizar un proceso de ingeniería inversa de la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Se abstendrá de comprometer intencionadamente la seguridad de los servicios de certificación.
- Se abstendrá de utilizar las claves privadas correspondientes a las claves públicas incluidas en los certificados con el fin de firmar un certificado como si desempeñara la función de una Autoridad de Certificación.
- Los suscriptores de certificados cualificados que generen firmas digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales firmas electrónicas son equivalentes a firmas manuscritas, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de firma electrónica), según las disposiciones del Reglamento eIDAS.
- Los titulares de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Los titulares de certificados cualificados que generen sellos digitales utilizando la clave privada correspondiente a la clave pública incluida en el certificado deben asumir que tales sellos digitales gozan de presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté

vinculado, siempre que se utilice un dispositivo criptográfico (dispositivo cualificado de creación de sello electrónico), según las disposiciones del Reglamento eIDAS.
- Abonar las tarifas por los servicios de certificación y sellado de tiempo solicitados en los términos y condiciones previstos por la CA, cuando el titular coincida con el suscriptor.
- Autorizar a la CA a que, a través de la RA, utilice los datos personales aportados por el titular para validar, comprobar y autenticar la identidad declarada por este.
- Solicitar la modificación/renovación/suspensión/revocación del Certificado cuando se cumpla alguno de los supuestos previstos en las políticas y prácticas específicas y en la legislación vigente para los diferentes status del ciclo de vida de los certificados
- Comprender y aceptar los términos y condiciones de uso del certificado, y cualquier modificación que se realice a estos
- No comprometer intencionalmente la seguridad de los servicios de certificación
- Todas las que se deriven de la DPC, la política de certificado específica y de la legislación vigente.

7.5.2.- Uso de la clave pública por la parte que confía y uso del certificado

Los terceros que confían en los certificados expedidos por EADTrust deben verificar la validez de los certificados y están sujetos a las siguientes obligaciones:

- Evaluar independientemente la idoneidad del uso de un certificado y determinar que, de hecho, se utilizará para un propósito apropiado.
- Ser consciente de las condiciones para usar los certificados de conformidad con lo establecido en la Declaración de Práctica de Certificación, y especialmente, en la PDS (Policy Disclosure Statement), es decir, la declaración abreviada para terceros que confían.
- Comprobar la validez, suspensión o revocación de los certificados emitidos, utilizando la información sobre el estado del certificado, disponible en el servicio OCSP.
- Comprobar todos los certificados en la jerarquía de certificados antes de confiar en una firma digital o en cualquiera de los certificados de la jerarquía. En relación con los certificados cualificados, comprobar que la autoridad de certificación raíz de EADTrust en cuya jerarquía se encuentra el certificado, está incluida en la lista TSL correspondiente[5].
- Tener en cuenta las limitaciones de uso de los certificados, ya estén contenidas en el propio certificado, en la PDS o en su caso, en el contrato de verificador.
- Tener en cuenta las precauciones incluidas en un contrato u otro instrumento, independientemente de su naturaleza legal.
- Notificar a EADTrust cualquier inexactitud o defecto en un certificado que pueda considerarse causa de revocación.
- Abstenerse de supervisar, interferir o realizar ingeniería inversa en la implementación técnica de los servicios de certificación sin la previa aprobación por escrito de la Autoridad de Certificación.
- Abstenerse de comprometer intencionalmente la seguridad de los servicios de certificación.
- Asumir que las firmas electrónicas cualificadas son equivalentes a firmas manuscritas, de conformidad con el artículo 25.2 del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Cada tercero que confía en los certificados expedidos por EADTrust al aceptar el uso de tales certificados reconoce:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

7.6.- Renovación del Certificado

[5] En España, la lista TSL la publica el Ministerio de Asuntos Económicos y Transformación Digital y está disponible en: https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

EADTrust no renueva los certificados emitidos con anterioridad. El suscriptor que posea un certificado vigente, próximo a expirar, podrá solicitar la emisión de un nuevo certificado. Para lo cual se seguirá el procedimiento técnico de emisión descrito en los apartados anteriores de esta Política.

7.6.1.- Circunstancias para la renovación del certificado

No Aplica.

7.6.2.- Quién puede solicitar la renovación

No Aplica.

7.6.3.- **Procesamiento de solicitudes de renovación de certificados**

No Aplica.

7.6.4.- **Notificación de una nueva emisión de certificado al suscriptor**

No Aplica.

7.6.5.- **Conducta que constituye la aceptación de un certificado de renovación**

No Aplica.

7.6.6.- **Publicación del certificado de renovación por la CA**

No Aplica.

7.6.7.- **Notificación de la emisión del certificado por la CA a otras entidades**

No Aplica.

7.7.- Modificación del certificado

Cualquier necesidad de modificación de certificados implicará una nueva solicitud, y llevará aparejado que se realice una revocación del certificado previo y una nueva emisión de certificado, con los datos corregidos.

7.7.1.- Circunstancias para la modificación del certificado

No Aplica.

7.7.2.- Quién puede solicitar la modificación del certificado

No Aplica.

7.7.3.- Procesamiento de las solicitudes de modificación del certificado

No Aplica.

7.7.4.- Notificación de la emisión de un nuevo certificado al suscriptor

No Aplica.

7.7.5.- Conducta que constituye la aceptación de un certificado modificado

No Aplica.

7.7.6.- Publicación del certificado modificado por la CA

No Aplica.

7.7.7.- Notificación de la emisión del certificado por la CA a otras entidades

No Aplica.

7.8.- Revocación del certificado

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de éste en función de alguna circunstancia distinta a la de su caducidad.

7.8.1.- Circunstancias para la revocación

Las circunstancias que se tomarán en cuenta para la revocación de certificados son las siguientes:

- La solicitud de revocación ha sido realizada por el firmante, la persona física o jurídica representada por el firmante, un tercero autorizado o una persona física que solicitó un certificado digital para una persona jurídica.
- Los datos de creación de firma del firmante o del prestador de servicios de certificación han sido comprometidos o si el firmante o un tercero han utilizado los datos de forma incorrecta.
- Cuando se haya emitido una orden legal o administrativa a tal efecto.
- La muerte del firmante o la extinción de la persona jurídica titular del certificado de sello, la incapacidad total o parcial imprevisible del firmante o de la persona jurídica representada por el firmante, la terminación de la representación, la disolución de la persona jurídica representada, el cambio en las circunstancias de la custodia o uso de los datos de creación de firma o de sello incluidos en los certificados expedidos a una persona jurídica.
- El caso de que EADTrust termine su actividad, excepto en los casos en que el firmante haya dado su consentimiento para que los servicios de gestión de certificados electrónicos sean transferidos a otro prestador de servicios de certificación.
- Cambio en los datos suministrados para obtener el certificado o modificación de las circunstancias verificadas para la emisión del certificado.
- Que haya perdido la clave privada asociada al certificado, que haya sido robada o no sea útil debido a daños en el soporte del certificado
- Una de las partes incumple sus obligaciones, como, por ejemplo, el pago.
- Se detecta un error en el procedimiento de emisión del certificado, ya sea porque uno de los requisitos previos no se ha cumplido o debido a problemas técnicos durante el proceso de emisión del certificado.
- Existe una amenaza potencial para la seguridad de los sistemas y para la fiabilidad de los certificados emitidos por EADTrust por razones distintas del compromiso de los datos de creación de firmas.
- Fallo técnico en la emisión o distribución de certificados o de la documentación asociada.
- Si EADTrust recibe una solicitud para la emisión del certificado y ya existe un certificado válido de la misma clase y unicidad, el certificado válido será revocado a petición del solicitante.

7.8.2.- Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse por

- El sujeto/Firmante.
- El Solicitante responsable.
- La Entidad u Órgano (a través de un representante de la misma).

- La RA o la CA autorizadas por EADTrust.
- Podrá realizarse de oficio si a EADTrust le consta por otra vía que se han producido circunstancias que hagan necesaria la revocación.
- En caso de licitaciones, la solicitud de revocación la podrán realizar las personas designadas en cumplimiento de los pliegos por el poder adjudicador.

Cualquier parte que confía que considere que sea necesario revocar un certificado deberá ponerse en contacto con EAD Trust indicando su motivación. EAD Trust considerará estas solicitudes en el marco de su proceso de gestión de incidentes y tomará la decisión que considere necesario, informando a los participantes según corresponda.

7.8.3.- Procedimiento para la solicitud de revocación

El solicitante de revocación puede ponerse en contacto con EADTrust y solicitar la revocación de un certificado. EADTrust le informará sobre cómo formalizar su solicitud.

El certificado puede ser revocado en cualquier momento y se debe revocar en todos los casos de pérdida o robo.

Se registra y archiva la solicitud de revocación autenticada y la información que justifica la revocación.

Si la revocación es solicitada por otra persona que no sea el solicitante, suscriptor o titular de la clave, antes o simultáneamente a la revocación, EADTrust informará al propietario de la clave del certificado y al suscriptor sobre la revocación de su certificado y especificando el motivo de la revocación.

El solicitante puede solicitar la revocación del certificado a través de los siguientes canales:

a) En línea, cumplimentando el formulario de solicitud de revocación disponible en la dirección www.eadtrust.eu
b) Por correo electrónico con solicitud firmada electrónicamente utilizando un certificado cualificado.
c) Por correo postal dirigido al domicilio de EADTrust, enviando la solicitud de revocación de certificado firmada y validada ante notario.
d) Por un sistema de entrega certificada cualificada que acredite la identidad del remitente, que debe coincidir con uno de los sujetos legitimados para solicitar la revocación.

Posteriormente, se le darán indicaciones al solicitante para que agende una cita con la Autoridad de Registro de EADTrust con el fin de verificar la identidad del solicitante de la revocación.

El proceso de verificación de la identidad del solicitante de la revocación podrá llevarse a cabo mediante personación ante la Autoridad de Registro o mediante verificación de identidad a distancia por videoconferencia.

Una vez comprobado que la solicitud de revocación cumple con los requisitos definidos en esta Política y en la Declaración de Prácticas de EADTrust, se procederá a la revocación del certificado.

En el caso de licitaciones se tendrán en cuenta las condiciones establecidas por el poder adjudicador.

7.8.4.- Periodo de gracia para comprobar certificados revocados

Una vez que la revocación haya sido debidamente procesada por la RA, la información de revocación estará disponible a través del servicio OCSP.

El período de precaución o período de gracia que corresponda aplicar para la validación de los certificados es el máximo tiempo transcurrido entre renovaciones de CRL (cuando se aplica este procedimiento para comprobar si un certificado está revocado).

En la relación de firmas electrónicas, este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (CertificateRevocationLists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol).

Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación. El período de gracia recomendado es de 24 horas.

En caso de que sea de aplicación una política **de firma** concreta, es responsabilidad del tercero que confía en los certificados expedidos por EADTrust la comprobación de que la Política de Firma aplicable es compatible con la Política de Certificación de EADTrust. Dos de las posibles políticas a aplicar, en España, son la de la Administración General del Estado[6] y la de la Administración de Justicia[7].

EADTrust mantiene, en las CRLs, información sobre certificados revocados hasta la fecha de caducidad. No obstante, mantendrá disponible, más allá de la fecha de caducidad, un repositorio de las CRLs anteriores que permitirá comprobar si un certificado se revocó antes de su fecha de caducidad con esa información histórica. Este repositorio mantendrá CRL de hasta 1900 días de antigüedad.

7.8.5.- Tiempo en el que una CA debe procesar la solicitud de revocación

Para los certificados de entidad final. El periodo de revocación desde que EADTrust o una RA tiene conocimiento autenticado de la revocación de un certificado, ésta se produce de manera inmediata, como máximo 10 minutos tras la finalización de la comunicación que da noticias de las razones de la revocación, incorporándose en la próxima CRL a emitir y en la base de datos de la plataforma de gestión que consulta el respondedor OCSP.

7.8.6.- Requisitos de comprobación de revocación para las partes que confían

La comprobación del estado de los certificados es obligatoria para cada uso del certificado, ya sea consultando el servicio OCSP o la lista de revocación de certificados (CRL).

EADTrust suministra información a los verificadores sobre cómo y dónde encontrar las CRL y el servicio OCSP correspondientes, en particular en el campo AIA (Authority Information Access) del certificado y en el campo "CRL Distribution Point".

7.8.7.- Frecuencia de emisión de la CRL

EADTrust emite inmediatamente una Lista de Revocación de Certificados (en adelante CRL, en inglés) en el momento en que se revoca un certificado.

La CRL contiene el tiempo estipulado para la emisión de una nueva CRL, aunque se puede emitir una CRL antes del tiempo indicado en la anterior. Si no hay revocaciones, la lista de revocación de certificados se regenera diariamente.

La CRL para los certificados de entidad final se emite cada 24 horas o como máximo 10 minutos más tarde desde que se confirma la revocación.
La CRL para los certificados CA (ARL) se emite cada 12 meses o cuando se produce una revocación.

Los certificados revocados que caducan no se mantienen en la CRL. No obstante, se publica cada día una CRL que se mantiene en un repositorio hasta un máximo de 1900 días. Además, se conservan todos los certificados caducados (revocados o no) en el registro interno de EADTrust por un período total de 10 años adicionales, contados desde la fecha de caducidad.

No se generan "Last CRLs". Si una CRL caduca y no se ha emitido otra en el período estipulado (fecha en el campo NextUpdate), no se emitirá ninguna posterior. En caso de que se revoque una CA, se revocarán todos los certificados y se emitirá una CRL con todos los certificados revocados.

[6] https://www.boe.es/boe/dias/2016/11/03/pdfs/BOE-A-2016-10146.pdf
[7] https://www.cteaje.gob.es/cteaje/PA_WebAppSGNTJCTEAJE/descarga/CTEAJE-GIS-707-Autenticaci%C3%B3n, %20Certificados%20y%20Firma%20electr%C3%B3nica.pdf?idFile=53f9d618-467b-4993-a7bd- 7d5ef69ab654

7.8.8.- Actualización de las CRLs

El tiempo máximo de latencia, es decir, el tiempo que transcurre tras la finalización de la comunicación que da noticias de las razones de la revocación, hasta que la información está disponible en el servicio OCSP o en la lista CRL se establece en 10 minutos.

7.8.9.- Servicios de estado de certificado

EADTrust proporciona a las Entidades Usuarias un servicio de comprobación de certificados en tiempo real basado en OCSP (Online CertificateStatusProtocol)[8].

Este servicio está disponible las 24 horas del día, los 7 días de la semana. Conforme establece el Reglamento (UE) 910/2014 eIDAS, este servicio se ofrece de manera gratuita.

7.8.10.- Recuperación de Certificados

EADTrust no contempla en ningún caso la recuperación de certificados. En caso de que el propietario de un certificado haya perdido el acceso al mismo, será necesario generar uno nuevo, revocando previamente el anterior.

8.- Perfiles de Certificado

8.1.- Perfiles de Certificados de Entidad Final

8.1.1.- Perfil de certificado cualificado de sello electrónico para persona jurídica

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único
signature		Sha256WithRSAEncryptio n ó ecdsa-with-SHA256 ó ecdsa-with-SHA384
issuer		Igual al campo Subject del certificado de la CA emisora
validity		4 años
subject		
serialNumber	Opcional	DNI/NIE en formato ETSI EN 412-1
Surname	Opcional	Apellidos
Givenname	Opcional	Nombre
CommonName		Nombre común
organizationIdentifier		<3 caracteres de tipo de identidad><país>- <identificador>. Ejemplo: VATES-B12312312
Organization Name		Nombre registrado completo
Country		País
OrganizationalUnit		Certificado de Sello de Entidad
subjectPublicKeyInfo		RSA 2048 mínimo ECDSA 256 bits (prime256v1) ó 384 bits (secpr384r1)
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
extendedKeyUsage		clientAuth, emailProtection

[8] IETF RFC 6960 Online Certificate Status Protocol – OCSP

subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41231
cpsURI		http://policy.eadtrust.eu
userNotice		European Agency of Digital Trust, S.L. Legal Person Qualified Certificate for Qualified Payment Service Provider.
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		15
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

* En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de sello** se cambia el OID 1.3.6.1.4.1.501.2.1.1.0.41231 por 1.3.6.1.4.1.501.2.1.1.1.41231 y el OID 0.4.0.194112.1.1 por 0.4.0.194112.1.3
** En caso de que la clave privada del certificado se encuentre en un **dispositivo cualificado de creación de sello** se añade el
campo QSCD

Este tipo de certificados se expiden bajo las jerarquías cualificadas no web de persona jurídica y admite diferentes variantes.

8.1.1.- Perfil de certificado cualificado de sello de órgano Nivel Medio/Sustancial

Campos/Extensiones	Crítico	Contenido
version		3
serialNumber		Número positivo único (menor de 20 octetos)
signature		Sha256WithRSAEncryption
issuer		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
validity		5 años (o menos)

Campos/Extensiones	Crítico	Contenido
subject		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF. SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
Surname	Opcional	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público). Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: "DE LA CAMARA ESPAÑOL - DNI 00000000G"
Givenname	Opcional	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: "JUAN ANTONIO"
CommonName		Denominación de sistema o aplicación de proceso automático. CN= p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
Organization Name		Denominación (nombre "oficial" de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
subjectPublicKeyInfo		RSA 2048 mínimo
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
Subject Alternate Names		

Campos/Extensiones	Crítico	Contenido
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		Tipo de certificado Tipo= SELLO ELECTRONICO DE NIVEL MEDIO (String UTF8) Size = 31 2.16.724.1.3.5.6.2.1 **Nombre de la entidad suscriptora** Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.2.2 **NIF entidad suscriptora** NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.3 **DNI/NIE del responsable (titular del órgano)** DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.2.4 **Denominación de sistema o componente** Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: "PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA". (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.2.5 **Nombre de pila (titular del órgano)** N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.6 Ej: "JUAN ANTONIO" **Primer apellido (titular del órgano)** SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.2.7 Ej: "DE LA CAMARA" **Segundo apellido (titular del órgano)** SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.2.8 Ej: "ESPAÑOL" **Correo electrónico** Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.2.9
extendedKeyUsage		clientAuth, emailProtection

Campos/Extensiones	Crítico	Contenido
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.0.41233
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel Medio/Sustancial. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero.
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.2
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl
authorityInfoAccess		
calssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcPDS		
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

8.1.2.- Perfil de certificado cualificado de sello de órgano Nivel Alto

Campos/Extensiones	Crítico	Contenido
version		3

Campos/Extensiones	Crítico	Contenido
serialNumber		Número positivo único (menor de 20 octetos)
signature		Sha256WithRSA Encryption.
issuer		Igual al campo Subject del certificado de la CA emisora Country Organization Organizational Unit Organization Identifier Common Name
validity		5 años (o menos)
subject		
serialNumber	Opcional	Número único de identificación de la entidad, aplicable de acuerdo con la legislación del país. En España, NIF. SerialNumber = p. ej: S2833002. Número secuencial único asignado por el prestador (Printable String)) Size [RFC 5280] 64
Surname	Opcional	Primer y segundo apellido, de acuerdo con documento de identidad (DNI/Pasaporte), así como su DNI (Ver Criterios de Composición del campo CN para un empleado público). Primer apellido, espacio en blanco, segundo apellido del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 80 p. ej: “DE LA CAMARA ESPAÑOL - DNI 00000000G”
Givenname	Opcional	Nombre de pila, de acuerdo con documento de identidad (DNI/Pasaporte) Nombre de pila del responsable del certificado (titular del órgano) de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 p. ej: “JUAN ANTONIO”
CommonName		Denominación de sistema o aplicación de proceso automático. CN= p. ej: “PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA. Nombre descriptivo del sistema automático. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
organizationIdentifier		Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
Organization Name		Denominación (nombre “oficial” de la organización) del creador del sello.
Country		Estado cuya ley rige el nombre, que será "España" por tratarse de entidades públicas.
OrganizationalUnit		SELLO ELECTRONICO

Campos/Extensiones	Crítico	Contenido
OrganizationalUnit		Denominación oficial de la unidad p. ej: SUBDIRECCION DE EXPLOTACION
OrganizationalUnit		Código DIR3 de la unidad p. ej: E04976701
subjectPublicKeyInfo		RSA 2048 mínimo
extensions		
issuerAltName		Igual al campo SubjectAlternativeNames de la CA Emisora
Subject Alternate Names		
Rfc822Name		Correo electrónico de contacto de la entidad suscriptora del sello. P. ej: soporte.afirma5@minhap.es
Directory Name		**Tipo de certificado** Tipo= SELLO ELECTRONICO DE NIVEL ALTO (String UTF8) Size = 31 2.16.724.1.3.5.6.1.1 **Nombre de la entidad suscriptora** Entidad Suscriptora = p. ej: MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS (String UTF8) Size = 80 OID: 2.16.724.1.3.5.6.1.2 **NIF entidad suscriptora** NIF suscriptora = NIF entidad suscriptora, p. ej: S2833002 (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.3 **DNI/NIE del responsable (titular del órgano)** DNI/NIE responsable= p. ej: 00000000G (String UTF8) Size = 9 OID: 2.16.724.1.3.5.6.1.4 **Denominación de sistema o componente** Nombre descriptivo del sistema de sellado automático, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Denominación sistema = p. ej: “PLATAFORMA DE VALIDACION Y FIRMA ELECTRONICA. @FIRMA”. (String UTF8) Size = 128 OID: 2.16.724.1.3.5.6.1.5 **Nombre de pila (titular del órgano)** N = Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.6 Ej: “JUAN ANTONIO” **Primer apellido (titular del órgano)** SN1 = Primer apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 OID: 2.16.724.1.3.5.6.1.7 Ej: “DE LA CAMARA” **Segundo apellido (titular del órgano)** SN2 = Segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte. (String UTF8) Size 40 En caso de no existir el segundo apellido, se dejará en blanco (sin ningún carácter). OID: 2.16.724.1.3.5.6.1.8 Ej: “ESPAÑOL” **Correo electrónico**

Campos/Extensiones	Crítico	Contenido
		Correo electrónico de la persona responsable del sello, p. ej: juanantonio.delacamara.espanol@mpr.es (String) Size [RFC 5280] 255 OID: 2.16.724.1.3.5.6.1.9
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Derivada del resultado de aplicar el hash a la clave pública del sujeto
authorityKeyIdentifier		Derivada del resultado de aplicar el hash a la Clave pública de la AC emisora
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.501.2.1.1.1.41233
cpsURI		http://policy.eadtrust.eu
userNotice		Ej: "Certificado cualificado de sello electrónico de Administración, órgano o entidad de derecho público, nivel alto. Consulte las condiciones de uso en " + URL de la DPC o, en su caso, documento legal de tercero
policyIdentifier		0.4.0.194112.1.3 (OID ETSI QCP-l-qscd)
userNotice		European Telecommunications Standards Institute. eIDAS European Regulation Compliant
policyIdentifier		2.16.724.1.3.5.6.1
cRLDistributionPoints		http://crl.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crl
authorityInfoAccess		
caIssuers		http://ca.eadtrust.eu/eadtrust-subca-<algoritmo><tamañoclave>eadlp<Año>.crt
ocsp		http://ocsp.eadtrust.eu
basicConstraint	Crítica	CA false
qcStatements		
QcCompliance		Indicación de certificado cualificado
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		Integer:=15 ([ETSI EN 319 412-5] describe el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este) OID 0.4.0.1862.1.3
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
QcSSCD		
QcPDS		

Campos/Extensiones	Crítico	Contenido
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

9.- Requisitos Empresariales y Legales

9.1.- Tarifas

EADTrust recibirá las contraprestaciones económicas correspondientes, de acuerdo con las tarifas aprobadas por su Órgano de Dirección.

Las tarifas se recogen en el documento de términos y condiciones para cada tipo de certificado o servicio.

En el caso de concursos y licitaciones podrán establecerse otros precios en cumplimiento de los pliegos publicados por el poder adjudicador.

9.2.- Consideraciones de protección de datos de carácter personal

Todos los datos correspondientes a las personas físicas están sujetos a la normativa sobre protección de datos de carácter personal. De conformidad con lo establecido en el Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), también conocido como RGPD.

En España, es de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre de 2018, de protección de datos personales y garantía de derechos digitales, también conocida como LOPD-GDD.

Conforme establece la citada legislación de protección de datos, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

Los siguientes datos son considerados información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección correspondiente.
- Claves privadas generadas y/o almacenadas por la Entidad de Certificación.
- Cualquier otra información que pudiera identificarse como “Información privada”.

Los datos recabados por el prestador de servicios electrónicos de confianza tendrán la consideración legal que corresponda a su naturaleza, siendo normalmente datos de nivel básico. La información confidencial de acuerdo con la normativa de protección de datos es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado. A estos efectos EADTrust considera pública y no confidencial la siguiente información:

- Los certificados expedidos.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el

cambio de estado.
- Las listas de revocación de certificados, así como el resto de informaciones de estado de revocación.

9.2.1.- Consentimiento para usar datos de carácter personal

EADTrust S.L informa de que los datos personales a los que tenga acceso en el marco de la prestación de sus servicios serán incorporados al registro de actividades de tratamiento del que es Responsable. EADTrust fundamenta el tratamiento de datos fundamentalmente en: el interés legítimo que tiene en responder solicitudes de información sobre sus servicios, la ejecución de un contrato o en el consentimiento expreso del titular del dato. Los titulares de datos pueden retirar ese consentimiento en cualquier momento.

Los datos recabados son los mínimos necesarios para la prestación de los servicios y se conservan por los períodos que establece la Ley. No se ceden a terceros, salvo obligación legal; ni se realizan perfiles o se toman decisiones automatizadas en base a estos datos.

EADTrust le informa igualmente que, en caso de solicitar los servicios amparados en esta DPC por vía telefónica, su voz podrá ser grabada durante las conversaciones telefónicas que mantenga con la Autoridad de Registro (AR) o la Autoridad de Certificación (AC), con el fin de permitir una tramitación segura de la solicitud de emisión o revocación de certificados. Previo a la grabación se le ofrecerá la información básica de protección de datos estipulada en el RGPD y se le recabará su consentimiento expreso. Los datos personales recabados por esta vía se incorporarán al registro de actividades de tratamiento del que es responsable EADTrust.

Cuando el servicio de emisión o revocación de certificados se provea en la modalidad de verificación y autenticación de identidad mediante video conferencia o videograbación, EADTrust requerirá captar la imagen y la voz del Solicitante. La base legal para este tratamiento es la ejecución del contrato de prestación de servicios en esta modalidad conforme dispone el artículo 6.1 b) del Reglamento General de Protección de Datos. Estos datos son necesarios para la adecuada prestación del servicio y se incorporarán al registro de actividades de tratamiento de EADTrust.

Para más información sobre el ejercicio de los derechos al amparo del RGPD y sobre el tratamiento de sus datos personales por EADTrust consulte la nota legal más extensa, incluida en: http://eadtrust.rgpd.de/

9.2.2.- Comunicación a terceros de datos de carácter personal

Los datos de carácter personal solo podrán ser comunicados a terceros, siempre que el titular del derecho lo consienta expresamente o por obligación legal de EADTrust.

9.3.- Responsabilidad contractual y extracontractual

9.3.1.- Limitación de responsabilidad

EADTrust no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del titular de un certificado.

EADTrust no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.

EADTrust no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.

EADTrust no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en esta Política si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.

EADTrust no será responsable del contenido de aquellos documentos firmados electrónicamente por los titulares de certificados.

EADTrust no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en esta Política y en la normativa de aplicación.

9.3.2.- Responsabilidades

EADTrust responderá en el caso de incumplimiento de sus obligaciones según se indica en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y en la normativa reguladora de los servicios electrónicos de confianza, así como en la presente Política.

EADTrust responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

La responsabilidad del prestador de servicios de confianza regulada en la ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.

Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.

Cuando EADTrust, como prestador cualificado de servicios de confianza, informe debidamente a los suscriptores con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.

De manera particular, EADTrust como prestador de servicios de confianza responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados electrónicos.

EADTrust como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.

9.3.3.- Entidad de registro

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los solicitantes y la comprobación de sus datos, con las mismas limitaciones que se establecen para la Autoridad de Certificación.

9.3.4.- Responsabilidades del titular de los certificados

El titular de los certificados asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

Así mismo el titular de los certificados se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios.

Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al titular del certificado, por ejemplo, mediante técnicas de OCSPStapling, es decir haciendo uso de la extensión “TLS CertificateStatusRequest”.

Un certificado (en el sentido de instrumento que contempla la gestión de una clave privada) es un documento personal e intransferible emitido por EADTrust. Su titular está obligado a su custodia y la del código PIN o clave que habilita su uso, y es responsable de la conservación del mismo. No puede cederlos a otras personas.

9.4.- Exención de responsabilidades de EADTrust

EADTrust no asume ninguna responsabilidad por perjuicios ocasionados en las siguientes circunstancias:

- En caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y esta Política.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por la infraestructura de Certificación de EADTrut.
- Ocasionados por el mal uso de la información contenida en el certificado.
- La Autoridad de Certificación no será responsable del contenido de aquellos documentos firmados o sellados electrónicamente ni de cualquier otra información que se utilice en un proceso de autenticación en la que esté involucrado un certificado emitido por ella.

9.4.1.- Perjuicios derivados del uso de servicios y certificados

A excepción de lo establecido por las disposiciones de la presente Política, y lo determinado por Ley, EADTrust no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros que confían en los certificados.

9.4.2.- Seguro de responsabilidad civil

EADTrust cuenta con un Seguro de Responsabilidad Civil adecuado a sus actividades, según lo dispuesto en la normativa reguladora de los servicios electrónicos de confianza.

9.4.3.- Quejas. Reclamaciones y jurisdicción

En caso de una queja del usuario o de un tercero interesado, este podrá dirigir su queja al mail: info@eadtrust.eu o por correo postal; aportando copia de su identificación; así como todos los documentos y toda la información que considere oportuna para fundamentar su queja.

La CA de EADTrust en un plazo de 48 horas le remitirá por la misma vía de comunicación utilizada por el solicitante, un informe fundamentado de respuesta.

El plazo definido anteriormente podrá ser extendido en caso de que la resolución de la queja revista complejidad para su solución. Esta ampliación será comunicada al usuario.

En caso de que el usuario no esté conforme con la resolución de la queja. Este podrá presentar una solicitud de recurso de apelación ante la Dirección General de EADTrust. Para ello solo deberá comunicarse vía e mail a info@eadtrust.eu , indicando en el asunto que se trata de un recurso de apelación, también podrá emplearse la vía del correo postal.

Para la resolución de apelaciones se seguirá el procedimiento descrito anteriormente.

Las reclamaciones dirigidas a EADTrust se gestionarán de forma directa para intentar llegar a un acuerdo que resuelva el incidente o, en su caso, comprobar si es una cobertura incluida en el seguro.

La actividad de EADTrust se rige por la Ley española y por los Tribunales de Madrid, salvo que el usuario ostente la condición de consumidor, lo que redundará en que se aplique la normativa de protección de consumidores.